CLOUDFLARE®

Guide de survie du fournisseur SaaS

L'essentiel des performances, de la disponibilité et de la sécurité des applications pour les fournisseurs SaaS

+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

Résumé

Gartner prévoit que le secteur des services cloud progressera presque trois fois plus vite que l'ensemble des services informatiques d'ici 2022, le SaaS constituant le segment le plus important de ce marché.[1] Les solutions SaaS font désormais partie intégrante de l'infrastructure d'entreprise, mais les fournisseurs SaaS opèrent sur un marché de plus en plus encombré. Une enquête menée au printemps 2018 sur l'ensemble du secteur a identifié 6 829 sociétés SaaS en compétition sur le marché.[2]

Pour se démarquer de cette concurrence intense, les fournisseurs SaaS doivent rapidement lancer leurs applications sur le marché et fournir aux utilisateurs finaux des performances optimales, une disponibilité continue, des fonctionnalités de pointe et une sécurité des données robuste, tout en maintenant des tarifs d'abonnements abordables et des coûts d'exploitation interne faibles.

PARTIE 1

Les clients ne tolèrent plus la lenteur ni les temps d’arrêt

À l'aube du millénaire, la capacité de concentration humaine était de 12 secondes; aujourd'hui, elle n'est plus que de huit secondes.[3] Les conséquences sont énormes pour les professionnels du marketing et de la publicité, mais aussi pour les développeurs Web et les fournisseurs SaaS. Les consommateurs numériques d'aujourd'hui exigent des sites Web, des applications et des API qui se chargent instantanément et ne sont jamais hors ligne. Conscient de cette réalité, Google utilise la vitesse de la page comme facteur de référencement pour la recherche sur ordinateur et sur mobile.[4]

La gravité des problèmes de performances varie considérablement, allant de quelques secondes de délai à l'application entière qui ne répond pas ou qui n'est pas disponible. Cependant, les plus petits problèmes peuvent avoir un impact visible sur les taux d'engagement et de conversion :

- Google a constaté qu'une augmentation de la latence des sites, comprise entre 100 et 400 millisecondes, présentait un impact notable sur le comportement des consommateurs[5]
- Les conversions baissent de 7 % pour une seule seconde supplémentaire de temps de chargement[6]
- Environ la moitié des utilisateurs mobiles attendent des applications qu'elles répondent en moins de deux secondes[7]

Optimiser les performances et garantir la disponibilité de l'application

Différents facteurs peuvent avoir une incidence sur les performances des applications SaaS, notamment la distance géographique entre le serveur d'origine de l'application et l'utilisateur final, la conception de l'application, les pics saisonniers de demande, la connectivité Internet des utilisateurs finaux ou encore les attaques par déni de service distribué (DDoS), où les pirates informatiques bombardent les serveurs de requêtes indésirables dans le but de les submerger. Il existe diverses méthodes permettant aux fournisseurs SaaS de relever ces défis.

Réseaux de distribution de contenu (CDN)

On estime que pour chaque 160 km de distance géographique entre les ressources d'une application ou d'un site Web et un utilisateur final, on ajoute une latence de 0,82 milliseconde.[8] Un réseau de distribution de contenu (CDN) est un groupe de serveurs répartis géographiquement et stratégiquement placés à des points d'échange entre différents réseaux. Ces serveurs mettent en cache le contenu statique en périphérie du réseau et le distribuent aux utilisateurs à partir du serveur CDN le plus proche de leur localisation. La majeure partie du trafic Web est aujourd'hui desservie par des CDN, y compris le trafic provenant de sites majeurs tels que Facebook, Netflix et Amazon.

Outre l'optimisation des temps de chargement, les CDN offrent les avantages suivants :

- **Coûts de bande passante réduits.** En mettant en cache le contenu statique en périphérie et en appliquant d'autres optimisations, telles que la compression et la minification des fichiers, les CDN réduisent la quantité de données que les serveurs d'origine doivent fournir.
- **Redondance et fiabilité.** Étant donné que les serveurs sont distribués, les CDN peuvent utiliser l'équilibrage de charge pour gérer les pics importants de demande, les défaillances matérielles et système et les attaques DDoS, garantissant ainsi la disponibilité permanente des applications.
- **Sécurité des données optimisée.** Les CDN permettent de garantir que les applications disposent des certificats TLS/SSL à jour pour chiffrer et protéger les données en transit.

Équilibrage de charge

L'équilibrage de charge répartit le trafic des applications sur plusieurs serveurs afin d'optimiser les performances. L'équilibreur de charge s'assure qu'aucun serveur n'est surchargé, et si un serveur tombe en panne, il redirige le trafic vers les serveurs restants. Les requêtes client peuvent être distribuées de manière séquentielle, acheminées vers le serveur avec le moins de connexions ou, comme dans le cas d'un CDN, géolocalisées vers le serveur le plus proche de l'utilisateur final.

Adoption des standards modernes du Web

En plus d'utiliser un équilibreur de charge et de fournir des actifs aussi proches que possible des utilisateurs finaux sur le plan géographique, les développeurs SaaS doivent s'assurer qu'ils utilisent les standards modernes du Web tels que HTTP/2, TLS 1.3 et IPv6. Ces standards sont plus efficaces que leurs prédécesseurs. Ils résolvent de nombreux problèmes inhérents aux anciennes normes et incluent un certain nombre de fonctionnalités permettant de réduire la latence et d'améliorer les performances et la sécurité des données. Par exemple, TLS 1.3 réduit la latence causée par la négociation TLS en supprimant une connexion aller-retour complète pour l'établissement de session ; le protocole IPv6 gère les paquets plus efficacement que IPv4 ; et HTTP/2 permet, entre autres, la compression et le multiplexage des en-têtes.

Optimisation de contenu

Les sites Web modernes sont plus volumineux que jamais. Depuis 2011, la taille totale des pages ne cesse d'augmenter.[9] Tout ce contenu statique lourd et non optimisé ajoute encore plus de temps de latence, en particulier sur les appareils mobiles, qui sont à l'origine de près de 60 % des recherches sur le Web.[10] Voici quelques-unes des meilleures pratiques d'optimisation de contenu :

- Conception adaptative pour régler automatiquement la manière dont le contenu est livré en fonction du périphérique de l'utilisateur final.
- Minification pour supprimer les espaces inutiles, les commentaires et autres contenus dans les ressources textuelles, telles que JavaScript, CSS et HTML. Cela permet de réduire la taille des fichiers jusqu'à 20 %.
- Configuration des serveurs pour compresser les ressources texte avant de les envoyer aux utilisateurs.
- Utiliser la mise en cache de stockage local sur les navigateurs et les appareils mobiles.
- Différer le chargement de JavaScript jusqu'à ce que le texte, les images et les polices aient été restitués.

PARTIE 2

Les applications SaaS sont des cibles majeures pour les cybercriminels

Dans le modèle de déploiement traditionnel d'application sur site, toutes les données étaient stockées et traitées dans les limites de l'utilisateur final, qu'il s'agisse d'un intranet d'entreprise ou d'un ordinateur individuel. En revanche, les applications et les services cloud stockent, traitent et transmettent une multitude de données sensibles du côté du fournisseur SaaS, notamment des informations commerciales confidentielles, des données financières et de santé, des identifiants de connexion et des informations personnelles identifiables (PII). Les fournisseurs SaaS doivent s'assurer que ces données sont protégées contre les accès non autorisés de pirates informatiques externes et d'éventuels collaborateurs malveillants.

De nombreux fournisseurs SaaS hébergent plusieurs applications client au sein d'une infrastructure partagée ; chaque fuite de donnée, incident de fiabilité ou attaque subie par l'infrastructure partagée entraîne des retombées négatives pour les autres clients. En 2017, Sabre Corporation a révélé que sa solution de réservation d'hôtels SaaS, utilisée par plus de 32 000 établissements, avait subi une violation. L'attaque a exposé des données de cartes bancaires appartenant aux clients de grandes enseignes hôtelières, dont Four Seasons, Loews Hotels et Hard Rock Hotels & Casinos.[11] Le président de Sabre, Clinton Anderson, a qualifié la violation de « jour de réveil. »[12]

Les conséquences potentielles d'une cyberattaque réussie incluent les perturbations de service, l'atteinte à la réputation de la marque, le désabonnement des clients, les pertes de revenus et les amendes réglementaires résultant de la non-conformité au RGPD et aux autres lois obligeant les entreprises à prendre les mesures adéquates pour sécuriser les données client. Les recours collectifs intentés par les victimes de violation de données contre Uber et MyFitnessPal sont en cours d'arbitrage.[13] Pour avoir tenté de dissimuler la violation, Uber a été condamné à une amende de 148 millions de dollars par les autorités américaines et à 1,2 millions de dollars supplémentaires par les autorités européennes. Si le RGPD avait été en vigueur au moment du piratage massif d'Uber, l'entreprise aurait pu se voir imposer une amende équivalente à 4 % de son chiffre d'affaires annuel, soit environ 260 millions de dollars.[14]

Sécuriser les applications SaaS

La surface d'attaque potentielle pour les applications cloud est vaste et comprend les portails de connexion, les DNS et solutions d'hébergement partagés, ainsi que les vulnérabilités des applications. Les fournisseurs SaaS peuvent également être attaqués de l'intérieur par des collaborateurs mal intentionnés ou négligents.

Attaques DDoS

Les attaques DDoS augmentent en fréquence, en taille et en intensité. Les attaques de taille supérieure à 100 Gbit/s ont augmenté de 967 % entre le premier trimestre 2019 et le premier trimestre 2018, et plus des trois quarts des attaques ont ciblé plus d'un vecteur.[15] De nombreuses attaques DDoS utilisent des « armées zombies » d'appareils IdO piratés, comme ce fut le cas lors des attaques de botnet Mirai contre le fournisseur DNS Dyn en 2016.[16] Parfois, les pirates informatiques utilisent des attaques DDoS pour détourner l'attention du personnel de sécurité et lancer un autre type de cyberattaque.

L'atténuation efficace des attaques DDoS nécessite une stratégie pluridimensionnelle associant des mesures de sécurité proactives et réactives. L'utilisation d'un réseau CDN et de l'équilibrage de charge permet d'absorber l'impact des attaques DDoS en répartissant le trafic sur plusieurs serveurs, tandis que des mesures de filtrage du trafic telles que la limitation du débit, la mise en liste blanche/noire d'adresses IP et le suivi des connexions bloquent les requêtes malveillantes tout en autorisant le trafic légitime.

Attaques visant le DNS

Les attaques DNS impliquent que des pirates informatiques prennent le contrôle des enregistrements DNS d'un site Web et redirigent les visiteurs vers un site malveillant, souvent conçu pour ressembler au site original et légitime. Ces attaques peuvent se déployer de l'une des trois manières suivantes : en installant des logiciels malveillants sur les machines des utilisateurs finaux qui remplacent leur configuration DNS ; en détournant une session d'utilisateur sur un réseau Wi-Fi public ; ou en volant les identifiants de connexion pour accéder aux enregistrements DNS du propriétaire du nom de domaine. Lorsque la cible d'une attaque est une application SaaS, l'objectif final du pirate est généralement de voler des données client ou de détourner des comptes client. Selon Verizon, environ un tiers des violations de données signalées semblent impliquer une attaque DNS.[17]

La meilleure défense contre les attaques DNS consiste à utiliser un service d'enregistrement DNS sécurisé et géré utilisant DNSSEC, un ensemble de protocoles de sécurité permettant de vérifier les enregistrements DNS à l'aide de signatures cryptographiques. En vérifiant que la signature d'un site correspond à son enregistrement, les résolveurs DNS peuvent authentifier l'origine des données envoyées à partir du serveur DNS.

Attaques par credential stuffing (infiltration des comptes)

Les tentatives de connexion par force brute, aussi connues sous le nom de « credential stuffing », utilisent une multitude d'identifiants de connexion compromis disponibles à la vente sur le Dark Web. Les pirates informatiques utilisent des logiciels de connexion et des proxy, généralement des botnets IdO, pour bombarder des sites Web et des applications SaaS avec ces combinaisons nom d'utilisateur/mot de passe. Étant donné que de nombreuses personnes utilisent les mêmes identifiants de connexion sur plusieurs sites et applications, il est probable que certains d'entre eux fonctionnent.

Environ 90 % des tentatives de connexion sur les sites e-commerce proviennent de credential stuffing ; les compagnies aériennes, les banques et les hôtels figurent également parmi les principales cibles de ce type d'attaque.[18] Les attaques continueront à se multiplier tant que les utilisateurs finaux continueront à utiliser les identifiants de connexion. Les contrôles techniques contre l'infiltration de comptes incluent l'obligation pour les utilisateurs finaux de résoudre des CAPTCHA et le déploiement de la limitation du débit, qui bloque les attaques en périphérie du réseau en configurant des règles personnalisées qui définissent les seuils de requêtes, les délais d'expiration et les codes de réponse.

Menaces internes

Les pirates externes ne sont pas les seules menaces à la sécurité des applications SaaS. Les initiés malveillants qui abusent délibérément de leur accès aux ressources de l'entreprise, ainsi que les collaborateurs négligents qui ne respectent pas les règles de sécurité et d'accès, constituent de graves menaces pour la sécurité des données. Une étude publiée par Nucleus Cyber en juillet 2019 a révélé que 60 % des organisations avaient subi au moins une attaque d'initié au cours des 12 derniers mois.[19]

Les fournisseurs SaaS doivent définir avec précision l'accès des utilisateurs aux applications internes, en appliquant le principe de moindre privilège : chaque collaborateur doit bénéficier uniquement de l'accès au système dont il a besoin pour effectuer son travail, et pas davantage. En outre, ils doivent se protéger contre le vol d'identifiants en mettant en œuvre des procédures d'authentification d'utilisateur telles que l'authentification multifacteur (MFA) et en surveillant en permanence les systèmes pour détecter les comportements anormaux.

Utilisation de charges malveillantes

Les charges malveillantes exploitent les vulnérabilités des applications à l'aide de méthodes telles que les injections SQL, le cross-site scripting et les inclusions de fichiers à distance pour exposer les données sensibles. Les fournisseurs SaaS doivent protéger leurs applications en déployant un pare-feu applicatif Web (WAF) pour identifier et bloquer les requêtes malveillantes. L'environnement de cyber-menaces étant dynamique, les règles WAF doivent être mises à jour régulièrement pour garantir la protection des applications contre les nouvelles menaces émergentes.

Interception de données client non chiffrées

Les charges malveillantes exploitent les vulnérabilités des applications à l'aide de méthodes telles que les injections SQL, le cross-site scripting et les inclusions de fichiers à distance pour exposer les données sensibles. Les fournisseurs SaaS doivent protéger leurs applications en déployant un pare-feu applicatif Web (WAF) pour identifier et bloquer les requêtes malveillantes. L'environnement de cyber-menaces étant dynamique, les règles WAF doivent être mises à jour régulièrement pour garantir la protection des applications contre les nouvelles menaces émergentes.

SSL n'est plus facultatif, mais son activation sur des domaines CNAME peut s'avérer délicate

SSL (Secure Sockets Layer) est un protocole de sécurité standard qui établit un lien chiffré entre un serveur et un client, comme par exemple un navigateur et un serveur Web (site Web). La version moderne du protocole s'appelle TLS (Transport Layer Security). Un site Web qui utilise SSL (TLS) présenta une adresse Web HTTPS.

Sans SSL, toutes les données transmises entre le navigateur et le serveur Web sont envoyées en texte brut, ce qui signifie que les pirates informatiques peuvent facilement les intercepter en transit. Pour éviter cela, les sites Web obtiennent un certificat SSL. Il s'agit d'un « passeport numérique » qui associe le serveur Web à une clé cryptographique et initie une session sécurisée avec le navigateur de l'utilisateur, garantissant le chiffrement de toutes les communications entre le navigateur et le serveur.

Aux débuts du protocole SSL, seules certaines pages d'un site Web étaient chiffrées, comme celles des paniers d'achat en ligne. Cependant, ces dernières années, les grandes sociétés de technologie ont exercé une pression croissante sur les développeurs Web et les fournisseurs SaaS pour qu'ils adoptent universellement le protocole HTTPS. Google a commencé à utiliser le chiffrement HTTPS comme facteur de référencement en 2014.[20] Ensuite, Google Chrome et d'autres navigateurs Web populaires ont commencé à afficher des avertissements de premier plan sur les sites Web desservis via des connexions HTTP, pour prévenir les visiteurs qu'elles n'étaient pas sécurisées.[21] À la suite de ces changements, le chiffrement SSL (TLS) est devenu une obligation de facto pour réaliser des affaires en ligne.

Toutefois, suite à l'adoption généralisée du protocole SSL sur le Web, un sous-ensemble important d'entreprises ont été laissées pour compte : les fournisseurs SaaS qui offrent à leurs clients la possibilité d'utiliser des domaines personnalisés pour les ressources en ligne destinées au public, comme des pages d'accueil, des sites Web, des portails d'assistance, etc.

Les fournisseurs SaaS hébergent généralement les sites des clients sur un sous-domaine de leur domaine principal : par exemple, entreprisecliente.fournisseursaas.com. Cependant, la plupart des entreprises

clientes ne veulent pas que cette URL soit visible pour leurs propres utilisateurs finaux ; l'URL comprend le nom d'une autre société, ce qui affaiblirait leur image de marque, perturberait les utilisateurs finaux et nuirait à leur référencement. Au lieu de cela, elles utilisent leur propre URL de marque, telle que entrepriseclientе.com ou support.entrepriseclientе.com, et utilisent un CNAME pour la diriger vers entrepriseclientе.fournisseursaas.com.

Malheureusement, il est extrêmement difficile d'activer SSL sur les domaines CNAME. Les fournisseurs de SaaS n'avaient traditionnellement que deux options. La première consistait à demander à leurs clients de configurer un proxy inverse sur leurs serveurs pour sécuriser la connexion, puis de transférer la requête au serveur du fournisseur SaaS. Cependant, cela demande énormément de temps, d'efforts et d'expertise technique de la part du client.

La deuxième option consistait pour le fournisseur SaaS à créer une solution interne automatisée ou manuelle, ce qui demande énormément de temps et d'efforts de la part du fournisseur SaaS, du client ou des deux. Les certificats SSL doivent également être déployés sur un réseau de distribution mondial à grande échelle et maintenus en permanence, ce qui requiert du temps, des efforts et des dépenses supplémentaires.

PARTIE 3

Les solutions de Cloudflare pour les performances et la sécurité des applications SaaS

Cloudflare permet aux fournisseurs SaaS de distribuer rapidement des applications sécurisées et hautement performantes, de réduire leurs coûts opérationnels et de se démarquer sur un marché saturé

Performances, disponibilité et optimisation de contenu

Le réseau Cloudflare est constitué de datacenters situés dans le monde entier. Chaque datacenter prend en charge l'ensemble des services de sécurité et de performance Cloudflare afin d'optimiser les performances Web sur son réseau. De la recherche rapide d'adresses Web à la distribution accélérée au serveur d'origine, Cloudflare accélère le trafic aux points clés de la vie d'une requête.

DNS Cloudflare : Cloudflare est le fournisseur de service DNS faisant autorité le plus rapide et le plus fiable au monde.[22] Cloudflare fournit un DNS géré rapide et sécurisé, sous la forme d'un service intégré à son réseau.

Le **CDN** Cloudflare couvre un réseau mondial de datacenters qui mettent en cache le contenu plus près des utilisateurs. Ainsi, les requêtes n'ont pas besoin de parcourir de longues distances pour atteindre les serveurs d'origine.

L'équilibrage de charge Cloudflare offre un équilibrage de charge local et global pour réduire la latence en équilibrant la charge du trafic sur plusieurs serveurs ou en acheminant le trafic vers la région la plus proche. Il comprend des **contrôles d'intégrité** avec basculement rapide pour réagir rapidement aux défaillances et permettre aux visiteurs de les éviter.

Cloudflare prend en charge les **derniers standards et protocoles Web**, notamment HTTP/2 et QUIC (HTTP/3) pour une transmission plus rapide des données de la couche application et TLS 1.3 pour un chiffrement SSL plus efficace.

Cloudflare Argo Smart Routing fournit du contenu Web dynamique sur les liaisons disponibles les plus rapides, ce qui accélère considérablement la livraison et améliore l'expérience de l'utilisateur final.

Cloudflare prend en charge l'utilisation des **échanges signés avec Google AMP** et l'attribution d'URL natives lors de l'affichage dans le viewer AMP.

Pour les applications mobiles, **Cloudflare Mobile SDK** propose une analyse des performances du réseau mobile pouvant être intégrée à toute application.

Cloudflare offre un certain nombre de fonctionnalités **d'optimisation des images**, avec notamment le redimensionnement d'image, Polish et Mirage. Le redimensionnement d'image permet aux clients d'optimiser les images en les redimensionnant, en les recadrant, en les compressant ou en les convertissant au format WebP, un format d'image plus récent conçu pour un chargement rapide.
Cloudflare permet également la **diffusion parallèle d'images progressives** pour accélérer l'affichage de plusieurs images sur une page.

Cloudflare propose différentes options pour optimiser les vidéos. **Cloudflare Stream** est une plate-forme de vidéo en ligne pour la diffusion de flux, et **Stream Delivery** garantit la distribution de vidéos la plus rapide possible. Cloudflare propose également une **accélération de diffusion simultanée** pour diffuser du contenu en direct.

La priorisation, ou l'ordre dans lequel les éléments d'une page Web sont chargés, fait une énorme différence en termes de vitesse de chargement des pages. **Rocket Loader** de Cloudflare optimise la hiérarchisation de tous les éléments devant être chargés avant que le JavaScript présent sur la page puisse être exécuté. Cloudflare prend également en charge la **priorisation HTTP/2** afin de contrôler la hiérarchisation des éléments de la page, évitant ainsi la hiérarchisation par défaut plus lente de la plupart des navigateurs. **BinaryAST pour JavaScript** est pris en charge par Cloudflare afin d'accélérer l'analyse syntaxique de JavaScript afin qu'elle s'exécute plus rapidement, ce qui est crucial pour la performance des pages Web dynamiques ou personnalisées.

Sécurité des données et des applications

Toutes les offres de Cloudflare proposent une **atténuation illimitée des attaques DDoS,** quelle que soit la taille de l'attaque, sans frais supplémentaires. La sécurité multicouche de Cloudflare combine plusieurs capacités d'atténuation DDoS en un seul service, évitant ainsi les perturbations causées par le trafic malveillant tout en laissant passer le trafic légitime. Avec une capacité de 30 Tbps, le réseau mondial de Cloudflare peut gérer toutes les attaques distribuées modernes, notamment celles qui ciblent l'infrastructure DNS.

Le **DNS Cloudflare** utilise DNSSEC pour vérifier les enregistrements DNS à l'aide de signatures cryptographiques, protégeant ainsi les applications SaaS des attaques DNS. Cloudflare propose également **1.1.1.1,** un résolveur DNS public qui maintient la confidentialité des requêtes DNS.

Cloudflare offre un contrôle précis avec la **rate limiting** pour détecter et bloquer les attaques par infiltration de comptes en périphérie du réseau, et la gestion des robots pour détecter les **robots malveillants** utilisés pour les infiltrations de compte et autres cyber-attaques comme le spam de contenu et l'accumulation de stocks.

Cloudflare Access aide les fournisseurs SaaS à atténuer les menaces internes en leur permettant de sécuriser, d'authentifier et de surveiller avec précision l'accès des utilisateurs à n'importe quel domaine, application ou chemin sur Cloudflare. Cloudflare Access offre également une visibilité complète sur les connexions, les demandes d'accès et les modifications de politique récentes, afin que le personnel de sécurité puisse identifier les comportements suspects ou anormaux.

Le pare-feu **applicatif Web (WAF)** de niveau professionnel de Cloudflare protège les applications SaaS contre les vulnérabilités courantes comme les attaques par injection SQL, le cross-site scripting et la falsification de requêtes intersites. Le WAF de Cloudflare protège en permanence les applications contre les nouvelles menaces émergentes par le biais de mises à jour automatiques.

La **solution SSL pour SaaS** de Cloudflare facilite l'activation du protocole SSL (TLS) sur les domaines personnalisés CNAME de leurs clients et libère les fournisseurs SaaS et leurs clients du fardeau que représente la gestion des certificats SSL. En clôturant le protocole SSL au plus près des visiteurs Web, la solution de Cloudflare améliore aussi considérablement les performances par rapport aux solutions internes.

Livraison rapide des applications sur le marché

L'informatique sans serveur a le potentiel de créer des applications plus rapides et plus réactives que jamais en permettant aux développeurs de rédiger et de déployer du code sans tenir compte de l'infrastructure sous-jacente. **Cloudflare Workers** permet aux développeurs de créer des applications sans serveur qui s'exécutent sur le réseau de Cloudflare, plus près de vos utilisateurs. Les applications conçues avec Cloudflare Workers sont toujours disponibles, avec une réactivité à faible latence.

Conclusion

Aujourd'hui, les utilisateurs souhaitent des interactions plus personnalisées et plus rapides lorsqu'ils se connectent ou lancent une application. Avec les bons outils, il est possible de créer de telles expériences. Cloudflare contribue à l'accélération de plus de 190 millions de sites Internet, permettant ainsi aux entreprises d'offrir à leurs clients la meilleure expérience possible.

À propos de Cloudflare

La mission de Cloudflare, Inc. (www.cloudflare.com/fr-fr / @cloudflare) est de construire un Internet meilleur. Aujourd'hui, la société exploite l'un des plus vastes réseaux au monde, avec près de 10 % des entreprises du classement Fortune 1000 et environ 19 % des 10 000 plus grands sites Web utilisent au moins un produit Cloudflare. La plate-forme de Cloudflare protège et accélère tout type d'application en ligne sans installer de matériel, de logiciel et sans changer une ligne de code. Les sites Internet optimisés par Cloudflare voient leur trafic acheminé via notre réseau mondial intelligent, qui gagne en intelligence à chaque nouvelle requête. Ils profitent ainsi d'une amélioration significative de leurs performances, ainsi que d'une diminution du spam et des autres types d'attaques. En 2018, Cloudflare a été nommée sur la liste des meilleures cultures d'entreprise du magazine Entrepreneur et en 2019, elle a été classée parmi les entreprises les plus innovantes au monde par Fast Company. Le siège social de Cloudflare se trouve à San Francisco (Californie), avec des bureaux à Austin (Texas), Champaign (Illinois), New York, San Jose (Californie), Washington DC, Londres, Munich, Pékin, Singapour et Sydney.

Notes de fin

1. « Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, » Gartner Newsroom, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g. Consulté le 6 août 2019.

2. Smale, Thomas. « 4 Issues Facing the Saas Industry in 2019, » SaaS Magazine, https://saasmag.com/4-issues-facing-the-saas-industry-in-2019/. Consulté le 6 août 2019.

3. The Human Attention Span [Infographie], Digital Information World, https://www.digitalinformationworld.com/2018/09/the-human-attention-span-infographic.html. Consulté le 6 août 2019.

4. « Using page speed in mobile search ranking, » Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Consulté le 6 août 2019.

5. Brutlag, Jake. « Speed Matters, » Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. Consulté le 6 août 2019.

6. Rodman, Tedd. « Marketing & Web Performance: How Site Speed Impacts Metrics » Yottaa, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Consulté le 6 août 2019.

7. Dimensional Research. « Failing to Meet Mobile App User Expectations: A Mobile App User Survey, » https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. Consulté le 6 août 2019.

8. Sherman, Fraser. « Network Latency Milliseconds Per Mile, » Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile. Consulté le 6 août 2019.

9. Rapport : State of the Web, HTTP Archive. http://beta.httparchive.org/reports/state-of-the-web#bytesTotal. Consulté le 6 août 2019.

10. Sterling, Greg. « The mobile, desktop split may have stabilized at roughly 60% – 40%, » Search Engine Land, https://searchengineland.com/mobile-desktop-search-traffic-split-may-have-stabilized-at-roughly-60-40-317091. Consulté le 6 août 2019.

11. Hertzfeld, Esther. « New hotels caught in Sabre's data breach, » Hotel Management, https://www.hotelmanagement.net/tech/sabre-s-data-breach-affects-new-hotels. Consulté le 6 août 2019.

12. Taylor, Ian. « Sabre breach 'a wake-up call', ITB hears, » Travel Weekly, http://www.travelweekly.co.uk/articles/326108/sabre-breach-a-wake-up-call-itb-hears. Consulté le 6 août 2019.

13. « MyFitnessPal Data Breach Lawsuit Sent to Arbitration, » JD Supra, https://www.jdsupra.com/legalnews/myfitnesspal-data-breach-lawsuit-sent-49746/. Consulté le 6 août 2019.

14. Jones, Rhett. « Uber's Mountain of Data Breach Fines Just Got $1.2 Million Higher, » Gizmodo, https://gizmodo.com/uber-s-mountain-of-data-breach-fines-just-got-1-2-mill-1830679083. Consulté le 6 août 2019.

15. Rayome, Alison DeNisco. « Major DDoS attacks increased 967% this year, » TechRepublic, https://www.techrepublic.com/article/major-ddos-attacks-increased-967-this-year/. Consulté le 6 août 2019.

16. Dignan, Larry. « Dyn confirms Mirai botnet involved in distributed denial of service attack, » ZD Net, https://www.zdnet.com/article/dyn-confirms-mirai-botnet-involved-in-distributed-denial-of-service-attack/. Consulté le 6 août 2019.

17. Global Cyber Alliance, « The Economic Value of DNS Security, » https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. Consulté le 6 août 2019.

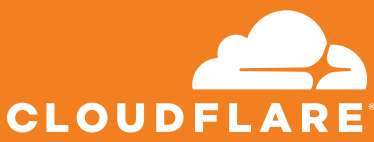
18. Detrixhe, John. « Hackers account for 90% of login attempts at online retailers, » Quartz, https://qz.com/1329961/hackers-account-for-90-of-login-attempts-at-online-retailers/. Consulté le 6 août 2019.

19. Bayern, Macy. « 60% of companies experienced insider attacks in the last year, » TechRepublic. https://www.techrepublic.com/article/60-of-companies-experienced-insider-attacks-in-the-last-year/. Consulté le 6 août 2019.

20. « HTTPS as a ranking signal, » Google Webmaster Blog, https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html. Consulté le 6 août 2019.

21. « Safari Says: Not Secure. What Does It Mean? » macReports, https://macreports.com/safari-says-not-secure-what-does-it-mean/. Consulté le 6 août 2019.

22. « DNS Performance Analytics and Comparison. » DNSPerf, https://www.dnsperf.com/. Consulté le 23 juillet 2019.



+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : 190812